## IN THE SPECIFICATION

Please replace the paragraph beginning at page 2, line 26 with the following amended paragraph:

In the Montgomery multiplication or the elliptic curve cryptography, algorithms of the arithmetic over GF(p) and the arithmetic over GF($2^n$) are substantially the same. Accordingly, when the arithmetic is implemented by circuits, data paths are mostly sharable without change except a multiplication core itself. The above-referenced J. Groszschaedl article discloses a multiplier ~~shearable~~ sharable by the arithmetic over GF(p) and GF($2^n$).

Please replace the paragraph beginning at page 6, line 14 with the following amended paragraph:

FIG. 7 is a diagram showing a structure of a multiplier ~~according to an embodiment~~, according to an embodiment of the present invention;